In the Specification

1. Please replace the first paragraph in the "Background Art" section on page 1 with the following amended paragraph:

Quantum key distribution involves establishing a key between a sender ("Alice") and a receiver ("Bob") by using weak (e.g., 0.1 photon on average) optical signals transmitted over a "quantum channel." The security of the key distribution is based on the quantum mechanical ~~principal~~ principle that any measurement of a quantum system in unknown state will modify its state. As a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the quantum signal will introduce errors into the transmitted signals, thereby revealing her presence.

2. Please replace the second paragraph in the "Background Art" section on page 1 with the following amended paragraph:

The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). Specific QKD systems are described in publications by C.H. Bennett et al entitled "Experimental Quantum Cryptography" J. Cryptology 5: 3-28 (1992), and by C.H. Bennett entitled "Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. Lett. 68 3121 (1992).

3. Please replace the last paragraph in the "Background Art" section on page 2 with the following amended paragraph:

While QKD is theoretically secure, the practical implementation of QKD allows for several ways for an eavesdropper to get information about the key bits. For example, to encode the value of a key bit on a photon one needs fast electronics, which produce electromagnetic radiation. This radiation can be measured by an eavesdropper in a so-

called "side channel attack." For phase-encoded QKD, this may be a serious problem, since phase modulators can actually produce enough measurable electromagnetic (EM) ~~EM~~ radiation. Second, an eavesdropper might get partial information on the key by monitoring transmission in the fiber. This is possible when multi-photon pulses are produced by a weak coherent source. An eavesdropper can measure such pulses without introducing errors in the transmission. Third, an eavesdropper may be able to launch a so called "Trojan horse attack" on Alice with a well-timed probing pulse in order to obtain information about the state of the phase modulator.

4. Please replace the third paragraph in the "Brief Description of the Drawings" section on page 2 with the following amended paragraph:

FIG. 3 is a flow diagram illustrating how Alice encrypts key bits produced by a random number generator by using a stream-cipher; and

5. Please replace the heading "Detailed Description of the Invention" on page 3 with the following heading:

Summary of the Invention

6. Please insert between the third and fourth paragraphs under the now re-named "Summary of the Invention" section on page 3, the following heading:

Detailed Description of the Invention

7. Please replace the first paragraph in the now-renamed "Detailed Description of the Invention" section on page 2 with the following amended paragraph:

FIG. 1 is a schematic diagram of a one-way QKD system 10 having a sending station Alice and a receiving station Bob. Alice and Bob are more generally sometimes referred to as QKD stations. Alice includes a controller 20 having a TRNG 30 and an encryption/decryption (e/d) module 40 connected thereto. Alice also includes an optical

radiation source 50 (e.g., a laser) and a polarization or phase modulator PM1 arranged downstream of the optical radiation source and optically coupled thereto. PM1 is operably coupled to e/d module 40, and laser 50 is operably coupled to the controller 20. In an example embodiment, optical radiation source 50 includes an attenuator (not shown) for reducing the intensity of optical pulses so that they are "weak," i.e., having single-photon level and below. In an example embodiment, optical radiation source is a single-photon source.

8. Please replace the fifth paragraph in the now-renamed "Detailed Description of the Invention" section on page 4 with the following amended paragraph:

With continuing reference to FIG. 1, in the normal operation of a QKD system such as QKD system 10, qubits are exchanged between Alice and Bob by controller 20 causing ~~laser~~ optical radiation source 50 to emit weak (e.g., ~0.1 photon) optical pulses. Controller 20 then provides basis and key bits via TRNG 30 (or alternatively via two separate TRNG's 30) to PM1 to randomly encode the weak pulses. At Bob, controller 120 also causes PM2 to randomly select (via TRNG 120) a basis to measure and detect the modulated qubits at detector 150.

9. Please replace the eighth paragraph in the now-renamed "Detailed Description of the Invention" section on page 5 with the following amended paragraph:

The method of encrypting Alice's key bits is illustrated in FIGS. 2 and 3. Suppose TRNG 30 generates basis bits ~~there are~~ b1, b2, ... bi,...bn ~~bits from TRNG 30 for basis~~ and key bits k1, k2, ... ki,...kn ~~bits~~ used to form a set of qubits. In an example embodiment, two TRNGs 30 are used to separately generate the basis and key bits, respectively.

10. Please replace the seventeenth paragraph in the now-renamed "Detailed Description of the Invention" section on the top of page 6 with the following amended paragraph:

Alternatively, Alice and Bob can run sifting and/or error correction first and decrypt